

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-87424

(P2003-87424A)

(43) 公開日 平成15年3月20日 (2003.3.20)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマート* (参考)
H 0 4 M 11/00	3 0 3	H 0 4 M 11/00	3 0 3 5 B 0 8 5
G 0 6 F 13/00	3 5 3	G 0 6 F 13/00	3 5 3 V 5 B 0 8 9
	5 1 0		5 1 0 A 5 K 1 0 1
15/00	3 1 0	15/00	3 1 0 D

審査請求 未請求 請求項の数11 O L (全 18 頁)

(21) 出願番号 特願2001-271802(P2001-271802)

(22) 出願日 平成13年9月7日(2001.9.7)

(71) 出願人 501120384

酒谷 信佳

神奈川県相模原市鞆野森1-18-18 サン  
シティイズミ204

(72) 発明者 酒谷 信佳

東京都文京区本郷1-25-2 明幸ビル6  
階 株式会社イー・ビジョン内

(74) 代理人 100104880

弁理士 古部 次郎 (外1名)

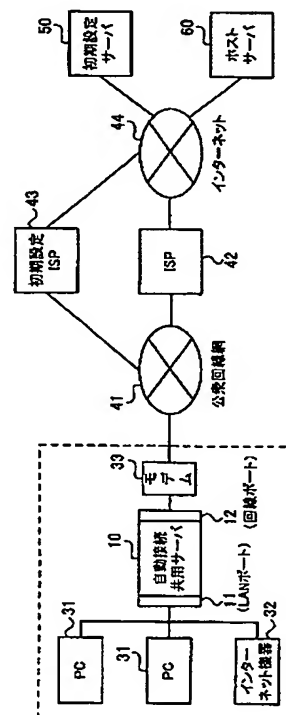
最終頁に続く

(54) 【発明の名称】 インターネット接続サーバ、初期設定サーバ、ホストサーバ、およびインターネット接続サーバの遠隔管理システム

## (57) 【要約】

【課題】 インターネットに接続する接続用サーバの設定を高い確実性で行い、また、障害などによりサービス提供不能に陥ったときであっても、容易に復旧させることができる。

【解決手段】 PC 31 やインターネット機器 32 を LAN 接続可能であると共にインターネット 44 に接続する自動接続共用サーバ 10 と、この自動接続共用サーバ 10 に予め設定された初期接続情報に基づいて接続される初期設定 ISP 43 と、自動接続共用サーバ 10 が本接続をするのに必要なネットワーク設定情報を保持する初期設定サーバ 50 とを備え、この初期設定 ISP 43 は、接続要求のあった自動接続共用サーバ 10 の接続認証を行い、認証できた場合にインターネット 44 に接続させ、この初期設定サーバ 50 は、初期設定 ISP 43 を経由して自動接続共用サーバ 10 にネットワーク設定情報を提供する。



## 【特許請求の範囲】

【請求項1】 複数の端末をLAN接続可能であると共に、インターネットに接続するインターネット接続サーバであって、

予め設定された初期接続情報に基づいて、初期設定用サーバとの接続を開始する接続開始手段と、

前記接続開始手段により接続が開始された前記初期設定用サーバから本接続に必要な設定情報を取得する設定情報取得手段と、

前記接続開始手段により開始された接続を切断する切断手段と、

前記設定情報取得手段により取得された前記設定情報に基づいて本接続を開始する本接続開始手段とを備えることを特徴とするインターネット接続サーバ。

【請求項2】 前記設定情報取得手段は、ユーザ契約しているインターネットプロバイダに対する接続情報を取得し、

前記本接続開始手段は、前記接続情報に基づいて前記インターネットプロバイダに接続することを特徴とする請求項1記載のインターネット接続サーバ。

【請求項3】 前記本接続開始手段により本接続が開始されたホストサーバからバージョンアップされたソフトウェアをダウンロードするダウンロード手段を更に備え、

前記ダウンロード手段によりダウンロードされた前記ソフトウェアにより動作することを特徴とする請求項1記載のインターネット接続サーバ。

【請求項4】 複数の端末をLAN接続可能であると共に、インターネットに接続するインターネット接続サーバであって、

予め設定された初期情報として前記インターネットに最初に接続するための情報が格納された不揮発性メモリと、

前記不揮発性メモリに記憶された情報に基づいて前記インターネットに接続されたサーバから得られたネットワーク設定情報を格納する書き込み可能記憶媒体とを備えたことを特徴とするインターネット接続サーバ。

【請求項5】 前記不揮発性メモリは、初期設定のためのインターネットプロバイダに対して仮接続を実行するための情報が格納されていることを特徴とする請求項4記載のインターネット接続サーバ。

【請求項6】 ユーザであるインターネット接続サーバ毎に固有な情報であるネットワーク設定情報を保持する設定情報保持手段と、

インターネット接続要求のあったインターネット接続サーバが、契約している正規のユーザであるか否かを確認するユーザ確認認証手段と、

前記ユーザ確認認証手段により正規のユーザであると判断された場合に、前記インターネット接続要求のあったインターネット接続サーバに対して前記設定情報保持手

段に保持された当該インターネット接続サーバのネットワーク設定情報を送信するネットワーク設定情報送信手段とを備えることを特徴とする初期設定サーバ。

【請求項7】 ユーザであるインターネット接続サーバを遠隔管理するホストサーバであって、前記インターネット接続サーバの動作に必要なソフトウェアと当該ソフトウェアの更新情報を保持するソフトウェア情報保持手段と、

所定のインターネット接続サーバからバージョン確認要求を受信する確認要求受信手段と、

前記確認要求受信手段によりバージョン確認要求のあった前記インターネット接続サーバに対して、前記ソフトウェア情報保持手段に保持されている最新のソフトウェアバージョン情報を送信するバージョン情報送信手段と、

前記インターネット接続サーバからの要求に基づいて、前記ソフトウェア情報保持手段に保持された所定のソフトウェアを提供するソフトウェア提供手段とを備えることを特徴とするホストサーバ。

20 【請求項8】 前記確認要求受信手段によりバージョン確認要求を受信した前記インターネット接続サーバが、契約している正規のユーザであるか否かを確認するユーザ確認認証手段を更に備えたことを特徴とする請求項7記載のホストサーバ。

【請求項9】 ユーザであるインターネット接続サーバを遠隔管理するホストサーバであって、所定のインターネット接続サーバから接続要求を受信する接続要求受信手段と、

30 前記所定のインターネット接続サーバが、契約している正規のユーザであるか否かを確認するユーザ認証確認手段と、

前記ユーザ認証確認手段により正規のユーザであると確認される場合にインターネット接続サーバのサービス構成情報を送信する送信手段とを備えることを特徴とするホストサーバ。

【請求項10】 複数の端末をLAN接続可能であると共にインターネットに接続するインターネット接続サーバと、

40 前記インターネット接続サーバに予め設定された初期接続情報に基づいて接続されるアクセスポイントを備える初期設定インターネットプロバイダと、

前記インターネット接続サーバが本接続をするのに必要なネットワーク設定情報を保持する初期設定サーバとを備え、

前記初期設定インターネットプロバイダは、接続要求のあった前記インターネット接続サーバの接続認証を行い、認証できた場合にインターネットに接続させ、

50 前記初期設定サーバは、接続要求のあった前記インターネット接続サーバが契約しているサーバであるか否かのユーザ確認認証を行い、認証できた場合に、前記初期設

定インターネットプロバイダを経由して当該インターネット接続サーバに前記ネットワーク設定情報を提供することを特徴とするインターネット接続サーバの遠隔管理システム。

【請求項11】 前記インターネット接続サーバは、前記初期設定サーバから前記ネットワーク設定情報が得られた後に、前記初期設定インターネットプロバイダとの接続を一時的に遮断し、当該ネットワーク設定情報に基づいて新たな接続を要求することを特徴とする請求項10記載のインターネット接続サーバの遠隔管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、インターネットへの自動接続サーバ等に係り、より詳しくは、ソフトウェアに障害が生じて自己で自動的に復帰させることができる自動接続サーバ等に関する。

【0002】

【従来の技術】 近年、数台のパソコンでLANを組み、それらをISDN経由でインターネットにダイヤルアップ接続する小規模ネットワーク用サーバから、企業内ネットワークやプロバイダのアクセスサーバとして使用される中・大規模ネットワーク用サーバまで、インターネットの接続共用サーバ(用途によってはルータと呼ばれている)が広く用いられている。

【0003】 また、従来の家庭用ネットワークや小規模ネットワークでは、インターネットに接続するときだけに公衆回線と接続するダイヤルアップ方式が採用されていた。しかし、近年では、回線使用料が安価となり、固定した定額料金でインターネットに接続するサービスを行うプロバイダや回線業者が出てきている。その結果、個人の家庭、小規模オフィスやマンション内のLANのように、比較的小規模であってもインターネットに常時接続できる環境が整ってきた。更に、PC以外のインターネットを利用する端末機器が出現してきており、家庭や小規模オフィスでも常時接続回線を複数の機器で共用するためのサーバが利用されるようになってきた。

【0004】 ところで、接続共用サーバは、ネットワークを相互に接続する機器であることから、インターネットにサーバを接続するために、最初に2つの手続き、即ち、モデムの設定とサーバの設定を行う必要がある。まず、モデムの設定では、公衆回線網、光ケーブル、無線回線、CATVなどと接続するための設定が要求される。サーバの設定では、ネットワーク番号と出力先ポートの対応表であるルーティングテーブルの設定が必要となる。更に、アドレス変換機能(NAT: Network Address Translation)や特定パケットの通過許可・禁止を行うフィルタリング機能に対応する設定も必要となる。

【0005】 ここで、中・大規模ネットワーク用サーバでは、ネットワークに対する知識の豊富な専門の担当者

(ネットワーク管理者)により管理されていることが多く、サーバに対する各種設定はこの担当者により行われている。また、接続後におけるサーバのメンテナンスもそのネットワーク管理者が担っている。かかる環境では、接続用サーバが故障したり、停電したりしてインターネットとの接続が不能になった場合には、担当者により、迅速にその復旧を図ることが可能である。また、中・大規模ネットワーク用サーバは、数百台程度が専用回線を用いて接続されており、モデムを使用せずに直接接続していることから、比較的、管理が容易であった。

【0006】

【発明が解決しようとする課題】 しかしながら、個人の家庭や小規模オフィス、或いはマンション内のLANのような環境では、接続共用サーバの設定を行うネットワーク管理者を置くことは容易ではない。上述のような設定作業は、ある程度の専門知識が必要であることから、一般ユーザには難しいものであり、個人のユーザが接続用サーバの設定を行うには困難が伴う。近年ではWebブラウザを用いて設定や運用ができるように工夫されているものも存在するが、それでも一般ユーザにとっては容易なことではない。機器提供者側にとっても、個々のユーザレベルに応じた運用・設定のためのインターフェースを用意することは非常にコストがかかる。

【0007】 更に、何らかの方法でリモートから管理することができたとしても、多数のサーバを同時に管理することは、ソフトウェアの多様性(インストールされるソフトウェアの組み合わせや、各バージョンが無数に存在する)の問題から非常に実現が難しく、結果的に1台1台個別に管理者などが対応していた。少なくとも数千台規模のサーバを保守するには、上記管理者の判断及び作業を安全に自動化する必要があった。

【0008】 また、今後、例えば電子レンジや冷蔵庫、オーディオ機器等の家電製品などを含め、PC以外の新しい機器がインターネットに接続され、提供されるサービスも無限に展開されると予想することができる。これらのニーズへの対応は、柔軟性の点から、一般に普及しているハードウェア型接続サーバでは難しい。そのために、ハードウェア型接続サーバの有する機能をリナックス(Linux)などの一般的なOSで実現するソフトウェア型接続共用サーバの利用も検討されている。このソフトウェア型接続共用サーバは、ハードウェア型接続サーバに比較すると柔軟で機能も豊富であるが、ソフトウェアに障害が発生した場合、煩雑な作業が必要であり、一般の個人ユーザでは、障害からの復旧が容易ではない。場合によっては、復旧するための設定情報をユーザが紛失すること考えられ、ユーザによる問題解決が困難であることが予想される。

【0009】 更に、インターネットへの常時接続用サーバの需要が個人ユーザの領域に広がっていくに従い、その設定をどのように行うかが問題となる。また、障害に

よってサーバとインターネットの接続が不能となったときに、その復旧を確実に行わなければならないが、その復旧作業を個人ユーザのレベルで容易に実施できないことが問題となる。

【0010】また、接続用サーバをインターネットに常時接続する場合には、外部からの不正アクセスを防御するためのファイアウォールが必要となる。通常は、簡易なファイアウォールとして、サーバのフィルタリング機能を利用し、セキュリティの確保が行われているが、今後、常時接続型の使用形態が個人ユーザにおいても盛んになり、大企業が採用するような本格的なファイアウォールの設定が必要になると予想される。しかしながら、このファイアウォールの設定にはより専門的な知識が必要とされ、さらに、進化する防御対策のためにファイアウォールのバージョンアップを定期的に行わなければならない。

【0011】このバージョンアップごとの接続用サーバの再設定や、接続用サーバの日常的な管理を行うことは、個人ユーザにとっては技術的に無理がある。更に、スケジューラの設定、インターネット制御によるテレビの設定などの新しい機能が加わった場合にも設定を変更しなければならず、新機能の追加やアップデートをするときにサーバの設定を失敗したときには、その対応が一般ユーザでは難しい。このような再設定や機能の変更は煩雑であるので、何らかの代行システムが望まれるところである。

【0012】本発明は、以上のような技術的課題を解決するためになされたものであり、インターネットに接続する接続用サーバの設定を確実性を高くして行うことができ、万一、障害などによりサービス提供不能に陥ったときであっても、容易に復旧させることができる自動接続サーバを提供するものである。

【0013】また、一旦、インターネットに接続用サーバを接続した後に、インターネットを介してそのサーバの管理を行うことにより、個人ユーザがサーバ設定を行わない場合であっても、ソフトウェアのバージョンアップや変更を行うことができる接続サーバの遠隔管理システムを提供することにある。

【0014】更には、ユーザ固有の情報をホストサーバに記憶し、様々なタイミング方法で同期させ、いつでも直前の状態に復帰させることができるシステムを提供することにある。

【0015】また更には、ユーザサーバの管理を自動化し、サーバにインストールされるソフトウェアの構成を管理パターンに限定することで、多数のサーバの一元管理、及び自動運転を可能にするシステムを提供することにある。

【0016】

【課題を解決するための手段】かかる目的を達成するために、本発明では、インターネットに接続するための設

定をユーザが考慮せずに立ち上げることによって自動的にインターネットに接続でき、何らかの原因でインターネット接続サーバ内のソフトウェアに障害が生じて、自己で自動的に復帰させることができるインターネット接続サーバを提供している。

【0017】即ち、本発明は、複数の端末をLAN接続可能であると共にインターネットに接続するインターネット接続サーバであって、予め設定された初期接続情報に基づいて初期設定用サーバとの接続を開始する接続開始手段と、この接続開始手段により接続が開始された初期設定用サーバから本接続に必要な設定情報を取得する設定情報取得手段と、接続開始手段により開始された接続を切断する切断手段と、取得された設定情報に基づいて本接続を開始する本接続開始手段とを備えることを特徴としている。

【0018】また、本接続開始手段により本接続が開始されたホストサーバからバージョンアップされたソフトウェアをダウンロードするダウンロード手段を更に備え、このダウンロード手段によりダウンロードされたソフトウェアにより動作することを特徴とすれば、自動接続した後のソフトウェアのバージョンアップやサービス内容をホストサーバと連携することで、効率的に自動運転することが可能となる。

【0019】また、他の観点から捉えると、本発明のインターネット接続サーバは、予め設定された初期情報としてインターネットに最初に接続するための情報が格納された不揮発性メモリと、この不揮発性メモリに記憶された情報に基づいてインターネットに接続されたサーバから得られたネットワーク設定情報を格納する書き込み可能記憶媒体とを備えたことを特徴としている。

【0020】ここで、この不揮発性メモリは、初期設定のためのインターネットプロバイダに対して仮接続を実行するための情報が格納されていることを特徴すれば、インターネットに接続するための設定を確実に行うことが期待できると共に、障害などにより接続不能に陥った場合でも再設定を容易に行うことができる点で好ましい。

【0021】また、本発明は、イニシャル時やトラブルからの再設定時等の初期設定時に接続される初期設定サーバとして捉えることができる。この初期設定サーバは、ユーザであるインターネット接続サーバ毎に固有な情報であるネットワーク設定情報を保持する設定情報保持手段と、インターネット接続要求のあったインターネット接続サーバが、契約している正規のユーザであるか否かを確認するユーザ確認認証手段と、このユーザ確認認証手段により正規のユーザであると判断された場合に、インターネット接続要求のあったインターネット接続サーバに対して設定情報保持手段に保持されたインターネット接続サーバのネットワーク設定情報を送信するネットワーク設定情報送信手段とを備えることを特徴と

している。

【0022】更に本発明は、本設定がなされた後にインターネット接続サーバを管理するホストサーバとして把握することができる。即ち、本発明は、ユーザであるインターネット接続サーバを遠隔管理するホストサーバであって、インターネット接続サーバの動作に必要なソフトウェアと当該ソフトウェアの更新情報を保持するソフトウェア情報保持手段と、所定のインターネット接続サーバからバージョン確認要求を受信する確認要求受信手段と、この確認要求受信手段によりバージョン確認要求を受信したインターネット接続サーバが、契約している正規のユーザであるか否かを確認するユーザ確認認証手段と、確認要求受信手段によりバージョン確認要求のあったインターネット接続サーバに対して、ソフトウェア情報保持手段に保持されている最新のソフトウェアバージョン情報を送信するバージョン情報送信手段と、このインターネット接続サーバからの要求に基づいて、ソフトウェア情報保持手段に保持された所定のソフトウェアを提供するソフトウェア提供手段とを備えることを特徴としている。

【0023】また、他の観点から把握すると、本発明が適用されるホストサーバは、所定のインターネット接続サーバから接続要求を受信する接続要求受信手段と、接続要求のあった所定のインターネット接続サーバが、契約している正規のユーザであるか否かを確認するユーザ認証確認手段と、このユーザ認証確認手段により正規のユーザであると確認される場合にインターネット接続サーバのサービス構成情報を送信する送信手段とを備えることを特徴としている。

【0024】一方、本発明は、インターネット接続サーバの遠隔管理システムとして把握することができる。このインターネット接続サーバの遠隔管理システムは、複数の端末をLAN接続可能であると共にインターネットに接続するインターネット接続サーバと、このインターネット接続サーバに予め設定された初期接続情報に基づいて接続されるアクセスポイントを備える初期設定インターネットプロバイダと、インターネット接続サーバが本接続をするのに必要なネットワーク設定情報を保持する初期設定サーバとを備え、この初期設定インターネットプロバイダは、接続要求のあったインターネット接続サーバの接続認証を行い、認証できた場合にインターネットに接続させ、この初期設定サーバは、接続要求のあったインターネット接続サーバが契約しているサーバであるか否かのユーザ確認認証を行い、認証できた場合に、初期設定インターネットプロバイダを経由してインターネット接続サーバにネットワーク設定情報を提供することを特徴としている。

【0025】ここで、このインターネット接続サーバは、初期設定サーバからネットワーク設定情報が得られた後に、初期設定インターネットプロバイダとの接続を

一時的に遮断し、このネットワーク設定情報に基づいて新たな接続を要求することを特徴とすれば、運営会社が管理する初期設定サーバでインターネット接続サーバの設定を行うことができるので、ユーザによる、サーバ（インターネット接続サーバ）のハードウェアやソフトウェアの設定を軽減することが可能となる。

#### 【0026】

【発明の実施の形態】以下、添付図面に基づき、本発明の実施の形態について詳細に説明する。図1は、本実施の形態が適用される自動接続共用サーバ遠隔管理システムの全体構成を示す図である。このシステムでは、例えば家庭用ネットワーク等の小規模ネットワークの中心に、ソフトウェア型自動接続共用サーバである自動接続共用サーバ10が設けられている。この自動接続共用サーバ10は、LANポート11を介してパーソナルコンピュータ(PC)31の他、インターネット44に接続可能なインターネット機器32（例えば、テレビジョン(TV)、冷蔵庫、クーラーなどの家庭用電化製品など）がLAN接続されている。また、自動接続共用サーバ10は、回線ポート12からモデム33を介して公衆回線網41に接続されている。

【0027】この公衆回線網41には、自動接続共用サーバ10のユーザが接続契約しているインターネットプロバイダ(ISP: Internet Service Provider)42と、初期設定のために接続契約しているインターネットプロバイダである初期設定ISP43が接続されている。ISP42は本接続用のインターネットプロバイダであり、初期設定ISP43は仮設定用のインターネットプロバイダである。このISP42および初期設定ISP43にはインターネット44が接続されており、インターネット44には、自動接続共用サーバ10の初期設定を行う初期設定サーバ50および自動接続共用サーバ10のメンテナンスを行うホストサーバ60が接続されている。この初期設定サーバ50およびホストサーバ60は、管理サーバ(ホスト側サーバ)として同一のサーバにより構成することも可能である。

【0028】また、公衆回線網41は、加入者電話網、ISDN、光ケーブル、無線回線、CATVなどのような形態が考えられる。また、自動接続共用サーバ10とインターネット44は、ダイヤルアップ接続環境または常時接続環境を構成しており、これらの何れであっても構わない。但し、以下の説明では、自動接続共用サーバ10の初期設定後は常時接続環境を前提としている。

【0029】まず、図1に示す自動接続共用サーバ10の内容について説明する。図2は、自動接続共用サーバ10の構成を示した図である。この自動接続共用サーバ10は、前述したLANポート11および回線ポート12を備えている。また、装置の全体を制御するCPU13、CPU13の動作プログラム等が格納されているPROM14、CPU13によって実行される各種プログ

ラムが利用する一時記憶領域であるRAM15、自動接続共用サーバ10を常時接続するために必要なプログラムや設定情報を記憶させるフラッシュメモリ16、補助記憶として各種情報を一時的に蓄積するHDD(Hard Disk Drive)17を備えている。

【0030】このPROM14は、電源を遮断しても記憶してある内容が消去されない不揮発性で、かつ回転など機械的動作を伴わず故障率が低いという性質から、自動接続共用サーバ10の動作として重要なプログラムや情報、即ち、全ての動作を処理するOSや初期接続情報等が記憶されている。このPROM14に記憶されている初期接続情報は、自動接続共用サーバ10における起動処理の他、異常時における復旧処理等に有効に機能する。

【0031】まず、読み出し専用記憶媒体に記憶されている内容について説明する。図3は、読み出し専用記憶媒体であるPROM14にて記憶されている内容を示した図である。このPROM14には、OS記憶領域21があり、このOS記憶領域21に格納されるOSとしては、例えばリナックス(Linux)などが挙げられる。また、後述するインストール管理プログラムが格納される。更に、PROM14には初期接続記憶領域22があり、自動接続共用サーバ10の電源を投入して立ち上げたときに最初に動作するプログラムとして、インターネット44に接続するために最小限必要なプログラム等(ブートプログラム、接続プロトコルなど)が格納されている。また、PROM14には初期接続情報記憶領域23があり、自動接続共用サーバ10が初期設定ISP43に最初に接続するために必要な情報(ドメイン名、ID番号、パスワード、サービスレベルなど)が記憶されていて、各々の自動接続共用サーバ10に固有の情報が振り分けられている。

【0032】尚、このPROM14のOS記憶領域21、初期接続記憶領域22、および初期接続情報記憶領域23に記憶された、OS、プログラム、固有の情報等は、自動接続共用サーバ10の出荷時に記憶されており、不揮発性メモリの特性により、通常の方法では消去することや書き換えることができないように構成されている。但し、簡単に消去されないようにソフトウェアを構成することによって、フラッシュメモリ16などを代用することも可能である。

【0033】自動接続共用サーバ10のRAM15は、電源の遮断によりその内容を消去する揮発性の性質を利用し、信号を順次記憶し、フラッシュメモリ16やPROM14に記憶されたプログラムが利用する一時記憶領域として利用されている。自動接続共用サーバ10の各種プログラムは、このメモリ空間上で実行される。

【0034】自動接続共用サーバ10のフラッシュメモリ16では、外部からの電圧により記憶してある内容を書き込み、また消去できる特性を利用し、自動接続共用

サーバ10を常時接続するために必要なプログラムや設定情報が記憶されている。このフラッシュメモリ16では、自動接続共用サーバ10を立ち上げた後に、初期設定サーバ50から本接続のために必要な情報やプログラムを読み込み、記憶させることができる。常時接続の後においては、必要に応じてホストサーバ60に接続し、フラッシュメモリ16に記憶させてあるプログラムを新しいバージョンに書き換えたり、追加することができる。

【0035】自動接続共用サーバ10のHDD17は、機械的な動作により信号を記憶し、フラッシュメモリ16と同様に外部からの指示により記憶してある内容を書き換えることができるという性質を有する。そこで、フラッシュメモリ16の代わりに、または、フラッシュメモリ16と共に、初期設定ISP43を介して取り込んだISP42の情報等を格納するように機能することができる。また、キャッシュ機能のために利用することが可能である。

【0036】このフラッシュメモリ16とHDD17は、何れかが選択的に設けられておれば足り、HDD17はフラッシュメモリ16と同等の役割を果たすことが可能である。両者が設けられている場合には、HDD17はフラッシュメモリ16の容量を補完するものとして利用される。

【0037】尚、自動接続共用サーバ10に、CD-ROMなどの可搬性のあるメディアの読み書き装置を設けることによって、大量のソフトウェアのダウンロードによって発生するネットワークトラフィックの削減と、ソフトウェアのUpdate等に要する時間を削減することができる。ユーザがCD-ROMを自動接続共用サーバ10に挿入すると、自動接続共用サーバ10内のPROM14におけるOS記憶領域21に格納されたインストール管理プログラムがCD-ROMの内容をチェックする。このインストール管理プログラムは、ホストサーバ60への接続を開始する。ホストサーバ60は、自動接続共用サーバ10にインストールされている改竄チェックプログラムを起動し、CD-ROMの内容を数値に変換して、ホストサーバ60にあらかじめ登録されている正規CD-ROMの計算値と同じであることを確認する。これは、不正なCD-ROMから不正なプログラムがインストールされることを防ぐために実施される作業である。計算値が異なった場合は、正規CD-ROMではないと判断し、CD-ROMをEjectする。正規CD-ROMであると認められる場合(CD-ROMの計算値とホストサーバ60に登録されている計算値が合致する場合)、ホストサーバ60は、ホストサーバ60に登録されているユーザのサービス構成を基に、新規サービスのインストール及び、ソフトウェアのUPDATEを実行している。

【0038】次に、書き込み可能記憶媒体に記憶されている内容について説明する。図4は、自動接続共用サー



バ10の書き込み可能記憶媒体(フラッシュメモリ16やHDD17)に記憶されている内容を示した図である。ここには、通常動作における基本ソフトウェアとして例えばリナックス(Linux)などからなるOS80、ソフトウェアのバージョンを確認して更新するバージョンチェックプログラム(VCP)81、ホストサーバ60から自動接続共用サーバ10が必要としているサービス情報を受信してその情報を書き換えるサービス構成プログラム(SCP)82、ネットワークの確立と設定を行うネットワーク構成プログラム(NCP)83が格納されている。

【0039】また、フラッシュメモリ16やHDD17には、外部からの攻撃や不正アクセスから内部ネットワークを守るファイアウォール(Firewall)84、改ざんをチェックするためのプログラムである改ざんチェックプログラム85、一度アクセスしたインターネットコンテンツを一時的に蓄積するキャッシュを管理するキャッシュ管理プログラム86を備えている。更に、ルータ機能を実行するIPルーティングプログラム87、インターネット44への接続を行うインターネット接続プログラム88、およびISP42に対する接続情報であるISP接続情報キャッシュデータ89を備えている。

【0040】例えばISP接続情報キャッシュデータ89を除く各種プログラム(80~88)は、自動接続共用サーバ10を出荷する初期段階に、自動接続共用サーバ10のフラッシュメモリ16やHDD17に格納することができる。ISP接続情報キャッシュデータ89は、仮接続の段階にて、初期設定サーバ50から取得されて格納される。但し、使用後、フラッシュメモリ16やHDD17に何らかの異常が生じてプログラムが消失した場合には、インターネット44を介して初期設定サーバ50やホストサーバ60から各プログラムをダウンロードして再構成することが可能である。

【0041】本実施の形態では、初期の接続では自動接続共用サーバ10から初期設定ISP43を経由し、インターネット44を介して初期設定サーバ50と仮接続し、自動接続共用サーバ10とモデム33の初期設定を行っている。次いで、自動接続共用サーバ10によりモデム33と公衆回線網41との接続を一時切断し、再度立ち上げて新しい接続情報によりモデム33とISP42を本接続させ、これ以降は常時接続の環境に維持させる。常時接続となった後では、自動接続共用サーバ10とホストサーバ60とをインターネット44を介して接続させ、必要に応じて適宜ホストサーバ60が自動接続共用サーバ10を遠隔管理している。

【0042】次に、図1に示す初期設定サーバ50について説明する。図5は、初期設定サーバ50の構成を示した図である。初期設定サーバ50には、基本ソフトウェアであるOS51の他、初期設定時に運営会社と契約している自動接続共用サーバ10か否かを確認するため

のプログラムであるユーザサーバ認証プログラム52、インターネット44に接続する前に、自動接続共用サーバ10に必要な個々の設定情報を記憶させるためのプログラムであるユーザサーバ設定情報取得プログラム53、および、ユーザサーバ設定情報取得プログラム53により取得された自動接続共用サーバ10毎に異なる接続のための設定情報が格納される自動接続共用サーバ管理テーブル55を備えている。

【0043】図6は、初期設定サーバ50の自動接続共用サーバ管理テーブル55に格納された情報の一例を示した図である。初期設定サーバ50の自動接続共用サーバ管理テーブル55には、それぞれの自動接続共用サーバ10ごとに異なった固有の各種設定情報が記憶されている。例えば図6に示すように、MAC(Media Access Control)アドレス、IP(Internet Protocol)アドレス、ドメイン、VPN(Virtual Private Network)、グローバルIP、その他の情報が保持されている。これらの設定情報は、各自動接続共用サーバ10によって相違しており、各自動接続共用サーバ10が固有に持っているMACアドレスなどによって識別されている。

【0044】次に、図1に示すホストサーバ60について説明する。ホストサーバ60は、自動接続共用サーバ10のメンテナンスを行っており、自動接続共用サーバ10の動作に必要なソフトウェアとその更新情報、重要度、各種ソフトウェア間の相性情報、ハードウェアとソフトウェアの相性情報などが記憶されている。ホストサーバ60側では、それらのソフトウェア、プログラムが随時、更新され、最新のバージョンのものが準備されており、適宜、自動接続共用サーバ10に供給できる体制にある。

【0045】図7は、ホストサーバ60の構成を示した図である。このホストサーバ60には、基本ソフトウェアであるOS61の他、新しいソフトウェアが出た場合に登録するためのプログラムであるソフトウェアアップデート管理プログラム62、インストールパターンにおけるデータの追加、変更、削除等を行うためのインストールパターン管理プログラム63、ソフトウェアの重要度を管理し、重要度が高ければアップデートを実施させるアップデート実施判断プログラム64、およびMACアドレスとパスワードを元に接続認証を行うユーザサーバ認証プログラム65を備えている。

【0046】また、ホストサーバ60では、例えばユーザが搭載しているソフトウェアのバージョン管理情報等、ユーザ情報を管理する自動接続共用サーバ管理テーブル66、最新ソフトウェアの管理情報やソフトウェアの重要度等が格納されるソフトウェアアップデート情報67、ソフトウェアのインストールパターンが格納されるインストールパターン管理テーブル68、およびダウンロードするためのソフトウェアの情報等が格納されるソフトウェアライブラリ69など、各種データが記憶媒

体に格納されている。

【0047】図8(a)～(e)は、ホストサーバ60に格納される各種情報の一例を示した図である。図8(a)に示す搭載ソフトウェアバージョン管理情報は、図7に示す自動接続共用サーバ管理テーブル66に格納される情報であり、各自動接続共用サーバ10は、Pattern\_IDを持っており、インストールパターン管理テーブル68とリンクされ、各ソフトウェアのバージョン情報が各自動接続共用サーバ10毎にMACアドレスによって管理されている。本実施の形態では、このPattern\_IDによっ

て、各自動接続共用サーバ10に搭載されているプログラムをパターン化している。

【0048】図8(b)に示される最新ソフトウェア管理情報および図8(c)に示される検証済みソフトウェアパッチ管理情報は、図7に示すソフトウェアアップデート情報67に格納されている。この検証済みソフトウェアパッチ管理情報では、重要度が管理されており、例えば重要度が5であればアップデートが行われ、その他であればアップデートは行わない等の処理に利用される。このように数値化することによってアップデートするかどうかの判断を自動化することができる。

【0049】図8(d)に示す検証済みソフトウェアインストールパターンは、図7に示すインストールパターン管理テーブル68に格納されている。このインストールパターン管理テーブル68は、各自動接続共用サーバ10にインストールされるソフトウェアのバージョンの組み合わせが有限個であることを示している。更に運営側で厳密に検証したパターンのみであれば、図8(e)に示すようなUpdateプログラム管理テーブルにより、そのパターン毎にUpdateプログラムを用意することによって、各自動接続共用サーバ10のUpdateを安全に自動化することができる。図8(e)に示すUpdateプログラム管理テーブルでは、1から4のパターンIDについて、夫々Updateプログラムが示され、夫々に優先度が示されている。

【0050】次に、本実施の形態が適用される自動接続共用サーバ遠隔管理システムの処理について、その流れを詳述する。まず、ユーザが自動接続共用サーバ10をインターネット44に接続する前に、そのユーザが使用する自動接続共用サーバ10に必要な個々の設定情報を初期設定サーバ50に記憶させておくことが必要である。本接続に必要な情報は、図6に示した、MACアドレス、IPアドレス、ドメイン、VPN、グローバルIP、その他の情報で、これらはユーザまたはISP42からメンテナンスの運営会社にFAXや電話、手紙などで通知しておく。メンテナンスの運営会社では、各自動接続共用サーバ10毎に異なる本接続のための設定情報を初期設定サーバ50に記憶させておく。この準備を行うことで、以下に説明する自動接続が可能となる。

【0051】図9は、自動接続共用サーバ10をインタ

ーネット44に自動的に接続させ、かつ、メンテナンスの管理を行うための基本的な処理手順を示す。まず、図1に示すようなシステム環境にて、LANケーブルが接続され、自動接続共用サーバ10の電源が入れられると、自動接続共用サーバ10のCPU13は、初期設定に基づいて自動接続プログラムを起動し、インターネット44を介して初期設定サーバ50に接続(仮接続)する(ステップ100)。次に、初期設定サーバ50から設定情報を取得し、ネットワークを再構成する(ステップ200)。この後、自動接続共用サーバ10は、ネットワークとの接続を一時切断し、新しい設定情報によって再度ネットワークに接続し直して、ホストサーバ60に接続(本接続)する(ステップ300)。

【0052】次に、自動接続共用サーバ10のCPU13は、バージョンチェックプログラム(VCP81)を起動し、自動接続共用サーバ10はホストサーバ60に接続して自分のマシンにインストールされているソフトウェアのパターンIDを取得し、Updateプログラム管理テーブルから対応する自動Updateプログラムをダウンロードし、その自動Updateプログラムを起動する。自動Updateプログラムは必要に応じてソフトウェアやアップデートパッチなどをダウンロードしながらUpdate処理を行う(ステップ400)。また、自動接続共用サーバ10のCPU13は、サービス構成プログラム(SCP82)を起動し、インターネット44を介してホストサーバ60から自動接続共用サーバ10のサービス構成情報を取得して、各サービスを起動する(ステップ500)。この一連の処理により、自動接続共用サーバ10の設定あるいは更新が完了し、ユーザは、自動接続共用サーバ10に接続されたPC31等からインターネット44にアクセスすることが可能となる(ステップ600)。

【0053】このインターネット44へのアクセスは、自動接続共用サーバ10の電源がOFFされるまで継続し(ステップ700)、常時接続環境を形成することになる。そして、電源がOFFされていない場合には、設定した時間が経過したか否かが判断され(ステップ800)、設定した時間が経過した場合、即ち、設定された一定の時間毎(例えば、1日に1回或いは1週間に1回)に、自動接続共用サーバ10はホストサーバ60に接続し直して、ステップ400からのルーチン処理を行い、最新バージョンのソフトウェアとサービス構成情報をダウンロードする。このため、自動接続共用サーバ10は、常時接続の環境にあっても最新バージョンのソフトウェアを使用することができ、ファイアオールやウイルスの対策も最新の情報に基づいて対処することができる。重要なセキュリティホールが発覚したような緊急を要する場合には、ホストサーバ60は、図6に示したような各自動接続共用サーバ10の固有の設定情報を参照し、必要と判断される自動接続共用サーバ10に接続して、自動接続共用サーバ10内のバージョンチェックプ



ログラム(VCP81)を強制起動する。

【0054】次に、図9に示した各ルーチンの詳細な処理手順について、図10～図13を用いて説明する。図10は、図9のステップ100における処理手順を示した図である。自動接続共用サーバ10の電源を投入すると、CPU13によりPROM14のOS記憶領域21に格納されているOSが起動し(ステップ101)、このOSで自動接続共用サーバ10が動作する。次いで、PROM14の初期接続記憶領域22に格納されている自動接続プログラムが自動的に起動する(ステップ102)。PROM14の初期接続情報記憶領域23には運営会社の特定の接続情報(電話番号またはIPアドレス等)が予め記憶されている。自動接続プログラムは、この隠れた接続情報により、予め設定されているインターネットプロバイダである初期設定ISP43のアクセスポイント(AP)に接続する(ステップ103)。このアクセスポイント(AP)は、メンテナンスの運営会社のものであり、自動接続共用サーバ10のユーザが契約しているインターネットプロバイダ(ISP42)ではない。この接続は初期設定の情報を入手するための仮接続となる。

【0055】次に、初期設定ISP43にて自動接続共用サーバ10の接続認証が行われ、認証ができた場合には、インターネット44との接続が許可される(ステップ104)。この認証は、PROM14の初期接続情報記憶領域23に記憶されたパスワード自動生成プログラム(自分のMACアドレスからホストサーバ60にある暗号キーを基に暗号化した値をパスワードとする)で生成したパスワード、MACアドレスを初期設定ISP43に送信することによって行われる。これにより、自動接続共用サーバ10の工場出荷時は、統一のプログラムをPROM14に記述すれば良く、各自動接続共用サーバ10毎に固有のパスワードなどを記録する必要がない。

【0056】自動接続共用サーバ10がインターネット44に接続された後、自動接続プログラムは、初期設定サーバ50との接続を開始する(ステップ105)。この接続では、運営会社と契約している自動接続共用サーバ10であるかどうかを確認するため、初期設定サーバ50にてユーザ確認認証が行われる。このユーザ確認認証は、自動接続共用サーバ10のPROM14の初期接続情報記憶領域23に記憶され、自動接続共用サーバ10から送信されたMACアドレス、ユーザID、パスワードなどにより行われる。初期設定サーバ50にて正規のユーザである自動接続共用サーバ10と認証されれば、初期設定サーバ50に接続される(ステップ106)。以上の処理により、自動接続共用サーバ10は、インターネット44を介して初期設定サーバ50に接続することができる。

【0057】図11は、図9のステップ200における

処理手順を示した図である。ステップ100で自動接続共用サーバ10と初期設定サーバ50のインターネット接続が完了すると、自動接続共用サーバ10のネットワーク構成プログラム(NCP83)が起動し、初期設定サーバ50に対してその自動接続共用サーバ10が必要としている設定情報の要求を出力する(ステップ201)。すると、初期設定サーバ50からは、その要求に応じて、自動接続共用サーバ10に特定された新しい設定情報が送信される(ステップ202)。この新しい設定情報は、前述した接続の準備段階において、予めユーザやISP42から電話、FAX、Eメール、Webページ(CGI Form)などの方法によって、自動接続共用サーバ10毎の情報として、初期設定サーバ50に記憶されている内容である。新しい設定情報は、図6に示されたものであり、初期設定サーバ50は、ユーザ確認認証により、対応した記憶領域にあるその自動接続共用サーバ10に必要な設定情報を呼び出すことになる。そして、送信された新しい設定情報は、自動接続共用サーバ10内のフラッシュメモリ16やHDD17に記憶される(ステップ203)。

【0058】図12は、図9のステップ300における処理手順を示した図である。自動接続共用サーバ10は、設定情報の記憶の処理が終わると、初期設定ISP43との接続を一時的に遮断し、インターネット44との仮接続を終了する(ステップ301)。その後、自動接続共用サーバ10内の自動接続プログラムが再起動し、書き換えられた新しい設定情報でインターネット44との接続を始める(ステップ302)。このときは、新しい設定情報により自動接続共用サーバ10が契約しているインターネットプロバイダであるISP42のアクセスポイント(AP)が選択される。ISP42は、接続要求のあった自動接続共用サーバ10の接続認証を行い、認証できたのであればインターネット44に接続させる(ステップ303)。この接続認証では、新しい設定情報によるもので行われ、例えばIPアドレス、MACアドレス、パスワードにより行われる。これ以降は本接続となり、その自動接続共用サーバ10が契約しているプロバイダ会社における専用のインターネットプロバイダであるISP42と継続して接続される。これ以降の接続は、常時接続環境であり、この環境は自動接続共用サーバ10の電源が切断されるまで続く。

【0059】自動接続共用サーバ10がISP42を介してインターネット44に接続された場合に、インターネット接続プログラム88は、最初にホストサーバ60との接続を要求する(ステップ304)。そして、ホストサーバ60では、接続要求をしてきた自動接続共用サーバ10であるかどうかを確認するため、ユーザ確認認証が行われる。ユーザ確認認証では、MACアドレスとユーザID、パスワードなどにより行われ、正規に契約したユ

ーザの自動接続共用サーバ10であれば、ホストサーバ60に開通することができる。以上の処理により、インターネット44を介して自動接続共用サーバ10とホストサーバ60との接続が完了する(ステップ305)。

【0060】自動接続共用サーバ10は、ホストサーバ60に接続して自分のマシンにインストールされているソフトウェアのパターンIDを取得し、Updateプログラム管理テーブルから対応する自動Updateプログラムをダウンロードし、その自動Updateプログラムを起動する。自動Updateプログラムは必要に応じてソフトウェアやアップデートパッチなどをダウンロードしながらUpdate処理を行う。

【0061】図13は、図9のステップ400における処理手順を示した図である。自動接続共用サーバ10とホストサーバ60との接続が完了すると、自動接続共用サーバ10のバージョンチェックプログラム(VCP81)が起動する(ステップ401)。そして、バージョンチェックプログラム(VCP81)がインターネット44を介してホストサーバ60へソフトウェアのバージョン確認の要求を送信する(ステップ402)。ホストサーバ60では、契約している自動接続共用サーバ10のユーザ確認認証が行われ、ホストサーバ60により自動接続共用サーバ10との接続が許可される(ステップ403)。

【0062】その後、ホストサーバ60では、接続された自動接続共用サーバ10のMACアドレスから、対象となる自動接続共用サーバ10に搭載されているソフトウェア/ハードウェアのPattern\_IDが取得される(ステップ404)。そして、Pattern\_IDからUpdateプログラム管理テーブルが参照され、パターンに適用すべきアップデート情報の重要度が確認される(ステップ405)。その結果、アップデートが必要か否かが判断され(ステップ406)、アップデートが必要な場合に、バージョンチェックプログラム(VCP81)は、Update Program管理テーブルに指定される自動アップデートスクリプトを自動接続共用サーバ10にダウンロードして、そのスクリプトを実行する(ステップ407)。自動アップデートスクリプトは、必要に応じてホストサーバ60等から新バージョンのソフトウェアをダウンロードする(ステップ408)。VCP81は、ダウンロードした自動アップデートスクリプトを使って自動接続共用サーバ10を最新状態にアップデートする(ステップ409)。VCP81から実行された自動アップデートスクリプトは、必要に応じてサービスの再立ち上げ、自動接続共用サーバ10の再起動を行う(ステップ410)。

【0063】一方、ステップ406で、アップデートが不要な場合には、バージョンチェックが終了し、自動接続共用サーバ10は、ホストサーバ60に対して準備が整った旨を通知する(ステップ411)。このとき、ホストサーバ60から自動接続共用サーバ10に接続できる

ように、ネットワーク情報などを通知してもよい。

【0064】尚、重要度とアップデート実施の判断については、例えば重要度5では、即アップデートが必要とされる。また、例えば重要度4では、早急なアップデートが必要であり、ネットワークの混み具合、自動接続共用サーバ10のその時点での利用率が高くない場合に実施されるものとして行うことができる。更に、例えば重要度3では、アップデートが必要であり、ネットワークが混んでおらず、かつ、ホストサーバ60と自動接続共用サーバ10との利用率が低いときに実施されるものとして行うことができる。このように、重要度に応じて、アップデート実施を判断することができ、重要度指数とその時点でのCPU使用率、ネットワーク使用率などの状況を見て判断するように構成することができる。

【0065】図14は、図9のステップ500における処理手順を示した図であり、管理会社のメンテナンス業務に対する処理である。インターネット44との本接続が完了すると、自動接続共用サーバ10のサービス構成プログラム(SCP82)が起動し(ステップ501)、インターネット44を介してホストサーバ60に接続される(ステップ502)。ホストサーバ60では、接続要求をしてきた自動接続共用サーバ10が運営会社と契約している自動接続共用サーバ10であるかどうかを確認するためユーザ確認認証が行われ、確認ができればその接続が許可される(ステップ503)。サービス構成プログラム(SCP82)は、ホストサーバ60からその自動接続共用サーバ10が必要としているサービス構成情報を受信し、その情報をフラッシュメモリ16に書き換える(ステップ504)。書き換えられたサービス情報により、自動接続共用サーバ10は、新しい内容で各サービスを起動して動作することになる(ステップ505)。

【0066】このサービスは、各自動接続共用サーバ10によって相違し、運営会社との契約内容によって相違するが、例えば、学校、企業、家庭等にて接続させたくないホームページを遮断させるためのコンテンツフィルタリングソフト、複数のパソコンで同時にインターネット接続を可能にするためのソフトウェアサーバ、外部からの不正アクセスを防御するためのファイアウォール、一度アクセスしたインターネットコンテンツを一時記憶しておき、再度同じコンテンツに接続する要求があったとき、蓄積したデータを自動接続共用サーバ10からPC31に提供するキャッシュサーバ、新しいウイルスが発見された時に、そのウイルスを除去するためのウイルスチェックソフトなどがある。自動接続共用サーバ10は、取得したサービス構成プログラム(SCP82)をフラッシュメモリ16に記憶し、このプログラムを基に自動接続共用サーバ10内の各サービスを起動する。

【0067】以上の処理は、停電などによってシステムダウンしたときなどに、必要に応じて起動され、自動接続共用サーバ10からホストサーバ60にアクセスする

ことにより、初期設定、アップデート、サービス構成情報の更新などを行うことができる。したがって、例えばシステムダウンした場合でも、電源のオン/オフのみで、システムダウン前の設定情報をホストサーバ60から取得し、復帰させることができる。この自動接続共用サーバ10の再起動では、初期接続に必要な情報はPROM14に全て記憶させてあり、しかもその記憶は不揮発性の性格であるため、物理的な破壊が無い限り必ず再起動することができる。また、障害が発生しても回復するために、初期設定等に必要となる時間と手間を少なくすることが可能となる。

【0068】また、ステップ500に示したサービス構成プログラム(SCP82)による書き換え、および更新は、一定時間毎に行うことができる。即ち、自動接続共用サーバ10とインターネット44の常時接続環境において、一定時間毎に(例えば1日に1回、あるいは1週間に1回)、自動接続共用サーバ10側からホストサーバ60にアクセスし、ソフトウェアのアップデートやサービス構成情報の更新を行うように構成しても良い。

【0069】次に、ユーザ側から自動接続共用サーバ10の設定情報を変更する場合について説明する。尚、自動接続共用サーバ10とインターネット44は常時接続環境にあるものとする。ユーザがネットワークの構成やサービスの設定を変更しようとする場合には、ユーザがPC31上のブラウザからホストサーバ60にログインする。そして、メールアドレスの作成や、ネットワークの設定情報の変更を行う。尚、ユーザが、FAXや電話で自動接続共用サーバ10を遠隔管理するメンテナンスの運営会社に変更内容を連絡し、メンテナンスの運営会社の方でホストサーバ60に対応する情報を設定しても良い。

【0070】ホストサーバ60は、上記のようにユーザから指定された情報を仮登録情報としてホストサーバ60内の自動接続共用サーバ管理テーブル66に記録する。ホストサーバ60は、この仮登録情報を元に自動接続共用サーバ10にアクセスし、設定情報の変更処理を行う。この設定変更処理が成功した場合、仮登録情報を本登録情報として自動接続共用サーバ管理テーブル66に再記録する。もし、この更新処理が失敗した場合でもホストサーバ60は、対象の自動接続共用サーバ10の状況を正確に把握することができるため、通常の復旧処理の後、続けて、先に失敗した更新処理を再度行うことができる。このように、自動接続共用サーバ10の設定変更は、ユーザが直接実施することではなく、メンテナンスの運営会社(例えば、ホストサーバ60)によって行われる。

【0071】次に、運営会社側から自動接続共用サーバ10の設定情報を変更する場合について説明する。尚、自動接続共用サーバ10とインターネット44は常時接続環境にあるものとする。ファイアウォールに新しいセ

キュリティホールが見つかった場合や、新しいサービスプログラムがリリースされた場合、新しいウイルスが見つかった場合などに、ホストサーバ60が管理している自動接続共用サーバ10で対象となる自動接続サーバを抽出し、順次アクセスし、自動接続共用サーバ10にインストールされているバージョンチェックプログラム(VCP81)を強制的に起動する。これにより、図9のステップ400の処理手順に従って、自動接続共用サーバ10からホストサーバ60にアクセスし、アップデートプログラムをダウンロードする。

【0072】次に、自動接続共用サーバ10におけるキャッシュサーバとしての働きについて説明する。図2に示すように、この自動接続共用サーバ10にはRAM15とHDD17が内蔵してある。これらはキャッシュサーバの作用を行うもので、RAM15とHDD17は、PC31がインターネット44を介して一度アクセスしたストリーミングデータを含むインターネットコンテンツを一時的に蓄積しておくことができる。PC31から再度同じコンテンツにアクセスする要求があった場合には、RAM15又はHDD17に蓄積したコンテンツを返却すれば良い。蓄積するコンテンツとオリジナルサーバにあるコンテンツの同期は、指定した期間ごとに自動的に行われたり、PC31側から要求がある度に同期の確認処理を行うことで、ユーザのPC31には最新のコンテンツを配信することができる。このキャッシュによるコンテンツの蓄積により、同じコンテンツを要求するためにインターネット44に通信する必要がなくなるため、通信回線の消費を節約でき、コンテンツのレスポンスの時間を短縮することができる。尚、例えば、HDD17にはキャッシュデータだけが記憶され、自動接続共用サーバ10の運営に重要なプログラムなどは記憶されないように構成することができる。そして、HDD17に記憶されたデータは何時でも消去できるようにすることができる。

【0073】次に、本実施の形態における変形例について説明する。図15は本実施の形態における第一の変形例を示した図である。この変形例では、自動接続共用サーバ10の初期設定でインターネット44に接続せず、専用の初期設定サーバ72で行うものである。公衆回線網41にはアクセスポイント(AP)71が接続しており、このAP71はメンテナンスの運営会社のものである。このAP71には初期設定サーバ72が専用回線などにより直結しており、初期設定サーバ72は図1で示した初期設定サーバ50と同様な機能を備えている。

【0074】この構成では、自動接続共用サーバ10の電源をオンすると、PROM14に記憶させた自動接続プログラムが起動し、公衆回線網41を介してモデム33をAP71に接続させる。AP71に接続されたならば、初期設定サーバ72は自動接続共用サーバ10の接続認証を行い、メンテナンス契約している自動接続共用

サーバ10であれば接続が許容される。この後、初期設定サーバ72は、自動接続共用サーバ10のために予め記憶させてあるネットワークの接続のための接続情報を送出する。自動接続共用サーバ10は、取得した新しい接続情報をフラッシュメモリ16に記憶させて、自動接続共用サーバ10とAP71の接続を一時切断し、仮接続を終了させる。そして、再度立ち上げて、新しい接続情報により自動接続共用サーバ10を立ち上げ、インターネットプロバイダ(ISP42)に接続し、本接続を開始させる。この後の処理は、図9のステップ300以下と同様となる。

【0075】図16は、本実施の形態における第二の変形例を示した図である。この変形例では、メンテナンスの運営会社が自動接続共用サーバ10の常時接続環境のプロバイダ会社を兼ねているような事例である。この場合、モデム33には、公衆回線網41を通じてインターネットプロバイダ(ISP42)に接続しており、ISP42は、インターネット44を介して初期設定兼用ホストサーバ73に接続される。この初期設定兼用ホストサーバ73は、図1におけるホストサーバ60と初期設定サーバ50の二つの能力を兼ね備えたものである。

【0076】この第二の変形例では、自動接続共用サーバ10の電源をオンすると、自動接続プログラムによりISP42のアクセスポイントに接続され、そのまま常時接続環境が設定される。次いで、自動接続共用サーバ10は、初期設定兼用ホストサーバ73に接続要求を行い、初期設定兼用ホストサーバ73は、ユーザ確認認証が完了すると予め記憶させてあるネットワーク設定情報を自動接続共用サーバ10に送出し、その後はソフトウェアのバージョンアップなどの処理を続けて行う。即ち、図9におけるフローでネットワーク接続の一時的な中断を行わずに、ステップ100からステップ500までの処理を一貫して実施することになる。

【0077】図17は、本実施の形態における第三の変形例を示した図である。この変形例では、自動接続共用サーバ10の回線ポート12に2つのモデム(モデム33およびモデム37)が接続され、モデム37には、公衆回線或いは専用回線を介してアクセスポイント(AP)74が接続され、更に、AP74には専用回線により初期設定サーバ50が接続されている。この第三の変形例では、自動接続共用サーバ10の電源を投入して立ち上げると、先ずモデム37によって自動接続共用サーバ10と初期設定サーバ50が接続され、インターネット接続に必要な接続情報を交信することができる。この構成であれば、モデム37は通信速度が低速度のモデムを使用でき、確実にAP74に接続することができる。

【0078】このように、本実施の形態が適用されるインターネット44への自動接続共用サーバ10では、初期接続に必要な接続情報は不揮発性の記憶回路(PROM14)に記憶させ、その情報によって最初の接続を行

うことができる。この最初の接続情報は、物理的な破壊によらなければ消去されることはなく、停電により自動接続共用サーバ10が一時動作を停止したり、何らかのソフトウェアの支障により故障したとしても、再度立ち上げることで自動的に接続させることができる。このため、専門の保守要員や技術者を配置せずとも、障害を克服することができ、何時でも再起動させることができる。また、個人の家庭や小規模の企業において常時接続型のサーバであっても、その復旧を自動的に行うことができる。

【0079】また、このサーバの遠隔管理システムでは、ユーザ側からすれば、運営会社が管理するホスト側サーバ(初期設定サーバ50およびホストサーバ60)でサーバの設定を行うことができるので、ユーザは自動接続共用サーバ10のハードウェアやソフトウェアの設定を行う必要がなく、インターネット44への接続からメンテナンスまで、常に最良の状態で自動接続共用サーバ10を維持管理していくことができる。また、自動接続共用サーバ10がシステムダウンした場合でも、ホスト側サーバ(初期設定サーバ50)にサーバの設定情報が保存されているので、簡単な再設定処理により容易にダウン前の状態に復旧させることができる。

【0080】一方、定期的に自動接続共用サーバ10からホストサーバ60にアクセスさせたり、あるいは常時接続環境においてホストサーバ60から自動接続共用サーバ10へのアクセスを可能とすることにより、運営側から各サーバ(自動接続共用サーバ10)の管理を一元的に行うことができ、サポートコストを大幅に低減することができる。また、各サーバ(自動接続共用サーバ10)のバージョンについてもホストサーバ60側で管理できるので、全サーバ(自動接続共用サーバ10)のバージョンアップにも簡単に対応させることができる。

【0081】このようにして、ユーザでは自動接続共用サーバ10をインターネット44に接続する際に、自ら初期設定の操作を行う必要がなくなる。そして、常時接続型の運転では、運営会社によりソフトウェアのバージョンアップやソフトウェアの変更、追加を自動的に行うことができ、ユーザは常に最新のソフトウェアでPC31やインターネット機器32を操作することができる。

【0082】

【発明の効果】このように、本発明によれば、インターネットに接続する接続用サーバの設定を高い確実性で行うことができる。また、万一、障害などによりサービス提供不能に陥ったときであっても、容易に復旧させることができる。

【図面の簡単な説明】

【図1】 本実施の形態が適用される自動接続共用サーバ遠隔管理システムの全体構成を示す図である。

【図2】 自動接続共用サーバの構成を示した図である。

【図3】 読み出し専用記憶媒体であるPROMにて記憶されている内容を示した図である。

【図4】 自動接続共用サーバの書き込み可能記憶媒体に記憶されている内容を示した図である。

【図5】 初期設定サーバの構成を示した図である。

【図6】 初期設定サーバの自動接続共用サーバ管理テーブルに格納された情報の一例を示した図である。

【図7】 ホストサーバの構成を示した図である。

【図8】 (a)～(e)は、ホストサーバに格納される各種情報の一例を示した図である。

【図9】 自動接続共用サーバをインターネットに自動的に接続させ、かつ、メンテナンスの管理を行うための基本的な処理手順を示した図である。

【図10】 図9のステップ100における処理手順を示した図である。

【図11】 図9のステップ200における処理手順を示した図である。

【図12】 図9のステップ300における処理手順を示した図である。

【図13】 図9のステップ400における処理手順を示した図である。

【図14】 図9のステップ500における処理手順を示した図である。

【図15】 本実施の形態における第一の変形例を示した図である。

た図である。

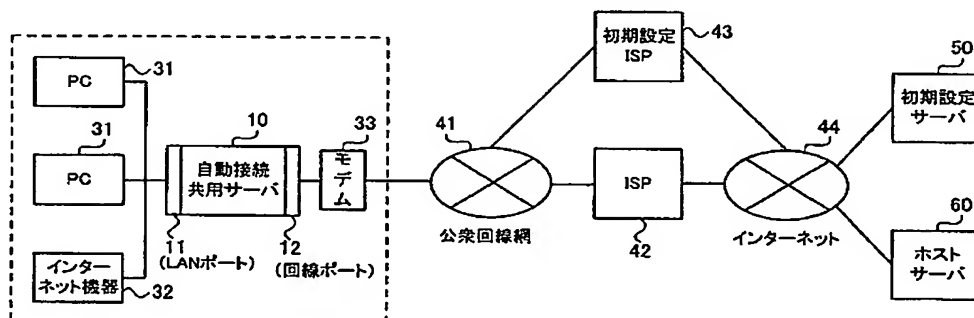
【図16】 本実施の形態における第二の変形例を示した図である。

【図17】 本実施の形態における第三の変形例を示した図である。

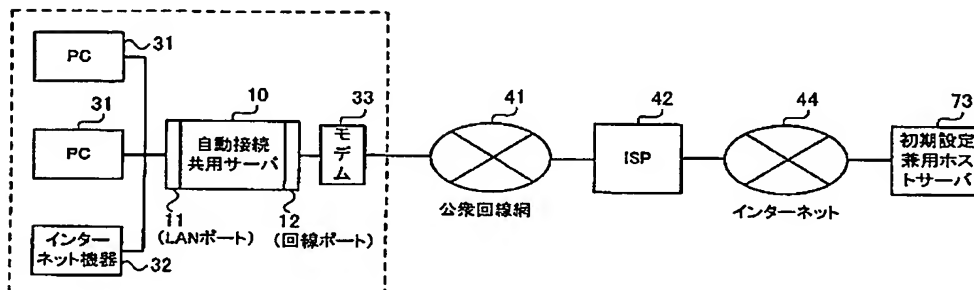
【符号の説明】

10…自動接続共用サーバ、11…LANポート、12…回線ポート、13…CPU、14…PROM、15…RAM、16…フラッシュメモリ、17…HDD(Hard Disk Drive)、21…OS記憶領域、22…初期接続記憶領域、23…初期接続情報記憶領域、31…パーソナルコンピュータ(PC)、32…インターネット機器、33…モデム、41…公衆回線網、42…インターネットプロバイダ(ISP)、43…初期設定ISP、44…インターネット、50…初期設定サーバ、51…OS、52…ユーザサーバ認証プログラム、53…ユーザサーバ設定情報取得プログラム、55…自動接続共用サーバ管理テーブル、60…ホストサーバ、61…OS、62…ソフトウェアアップデート管理プログラム、63…インストールパターン管理プログラム、64…アップデート実施判断プログラム、65…ユーザサーバ認証プログラム、66…自動接続共用サーバ管理テーブル、67…ソフトウェアアップデート情報、68…インストールパターン管理テーブル、69…ソフトウェアライブラリ

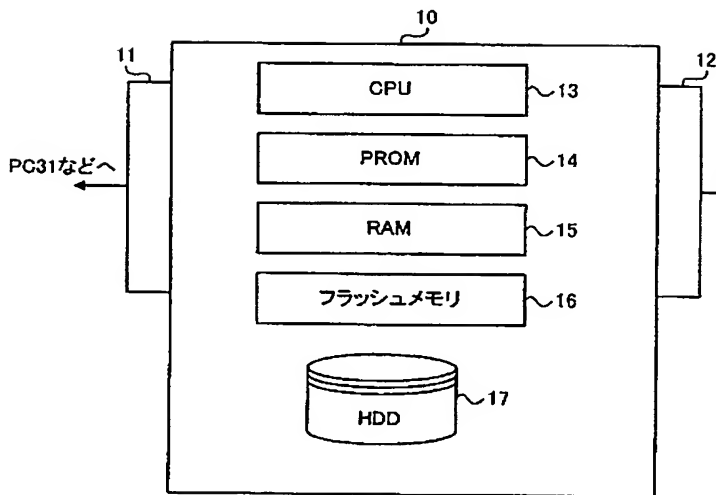
【図1】



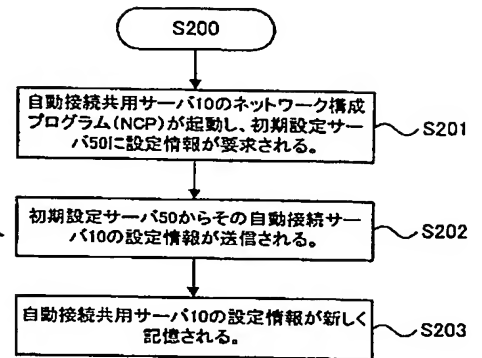
【図16】



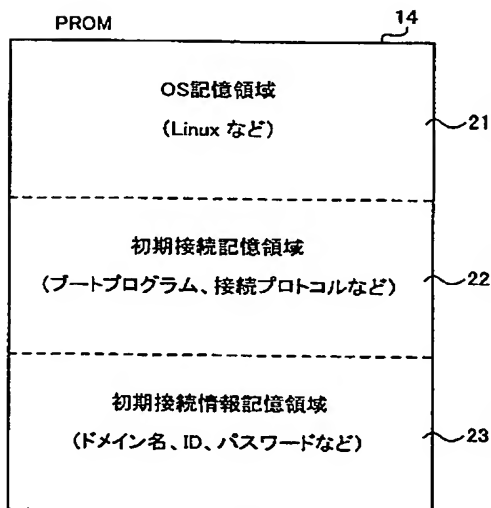
【図2】



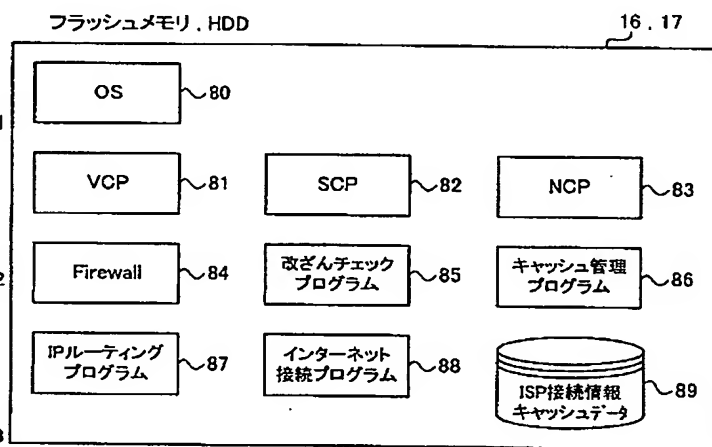
【図11】



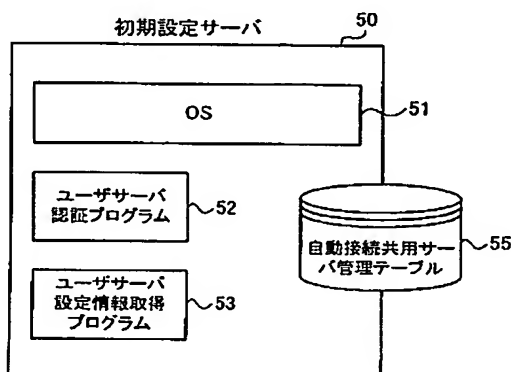
【図3】



【図4】



【図5】



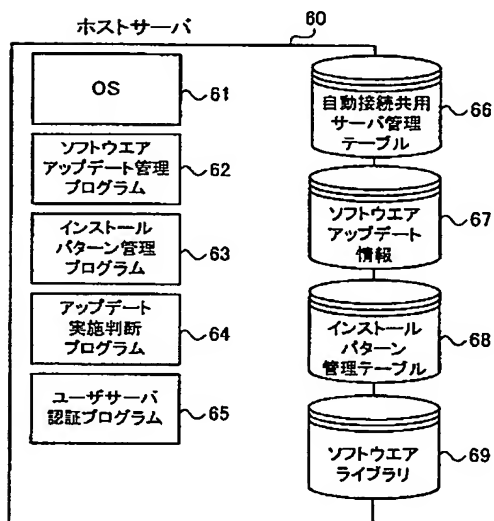


【図6】

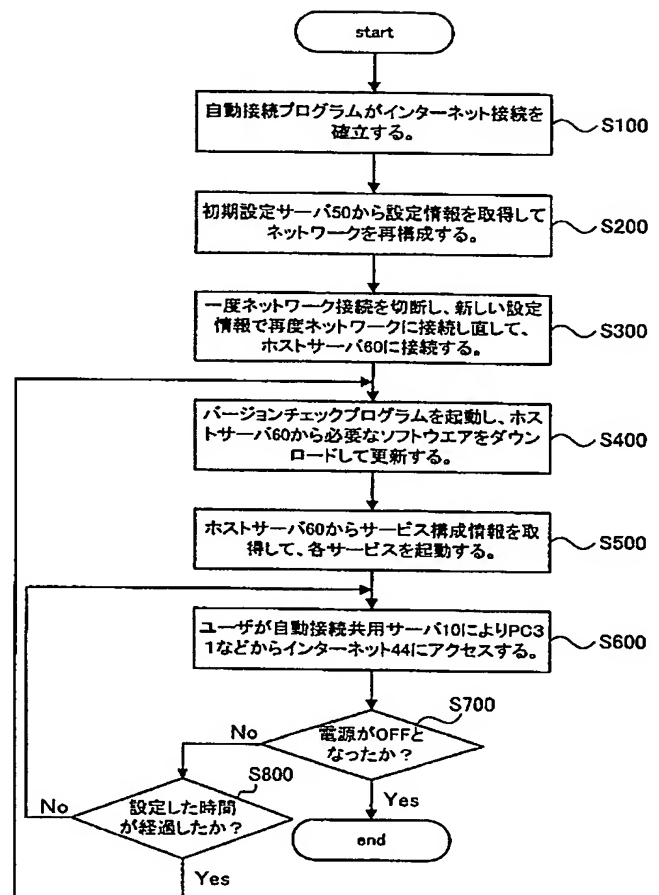
各家庭やオフィスに設置されるルータ(自動接続共用サーバ10)個々の設定情報。

MACアドレス	IPアドレス	ドメイン	VPN	Global IP	
XXXXXXXX	XXXXXX	XXXXXX	XXX	XXXXXXXXXXXX	
...	...	...	...	...	
XXXXXXXX	XXXXXX	XXXXXX	XXX	XXXXXXXXXXXX	

【図7】



【図9】



【図8】

## (a) 搭載ソフトウェアバージョン管理情報

MACアドレス	Pattern ID
01-00-E8-96-7F-E5	2
03-00-E5-67-8T-E4	3
90-02-SR-94-7V-D4	2
02-01-Z8-46-7T-G5	1

## (b) 最新ソフトウェア管理情報

AP ID	Name	最新Ver	Hardware Ver	OS Ver
1	FirewallX	8.1	1.1	5.8
2	Cach_man	4.5	1.1	5.8
3	IP_Sec	2.3	1.1	5.8
4	PPPoE	3	1.1	5.8
5	FirewallX	8.1	1.1	5.8
6	Cach_man	4.5	1.1	5.8
7	IP_Sec	2.3	1.1	5.8
8	PPPoE	3	1.1	5.8
~	~	~	~	~

## (c) 検証済みソフトウェアパッチ管理情報

Patch ID	Name	Ver	対象AP ID	重要度	OS Ver	Hardware Ver
1	FirewallX SecurityPatch	8.12	1	5	6.2	1.1
2	bug_fix	4.4	2	3	6.4	1.2
3	bug_fix	4.5	2	4	6.3	1.1
4	security_patch	2.8	3	1	7.1	1.2

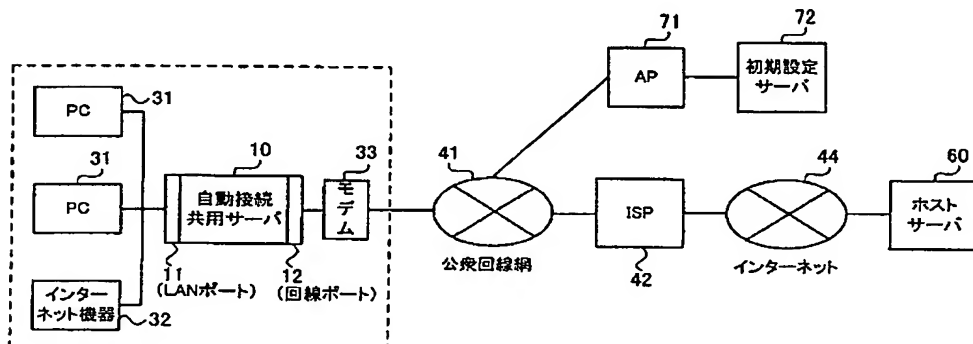
## (d) 検証済みソフトウェアインストールパターン

Pattern ID	AP1 ver	AP2 ver	AP3 ver	AP4 ver	OS Ver	Hardware Ver
1	2.4	3.4	6.1	7.1	6.2	1.3
2	2.3	3.2	5.8	7.1	6.2	1.2
3	2.3	3.2	5.8	7	5.8	1.1
4	2.3	3.3	5.8	6.7	5.8	1

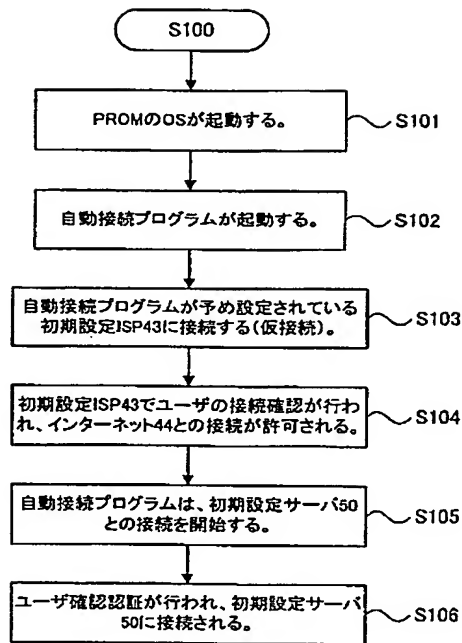
## (e) Update Program管理テーブル

Pattern ID	Update Program	重要度
1	/usr/prg/pat1_update.sh	3
2	/usr/prg/pat2_update.sh	2
3	/usr/prg/pat3_update.sh	2
4	/usr/prg/pat4_update.sh	1

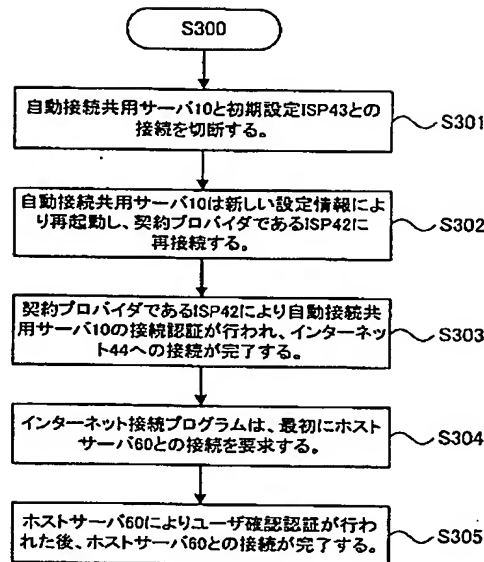
【図15】



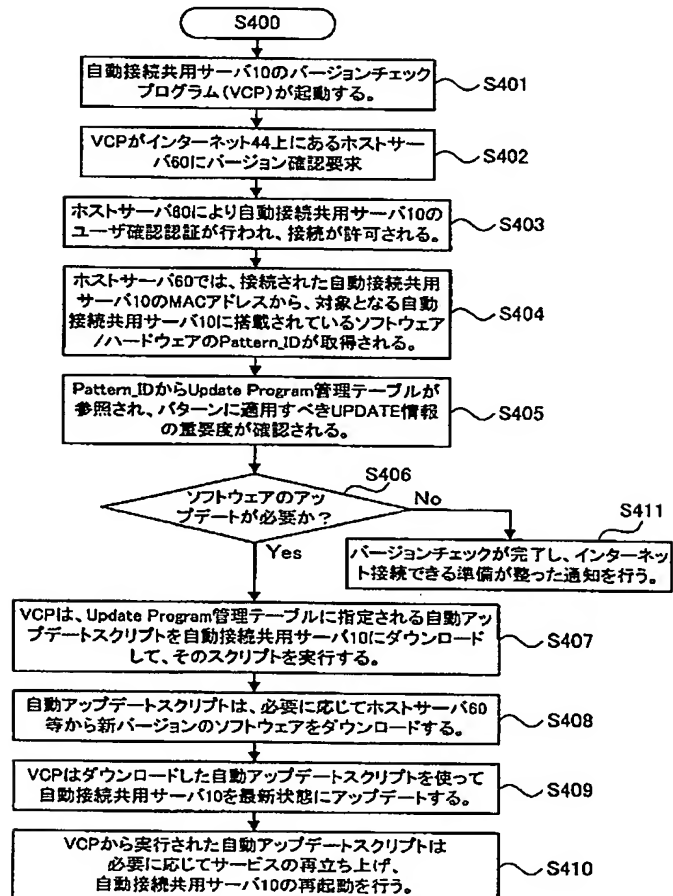
【図10】



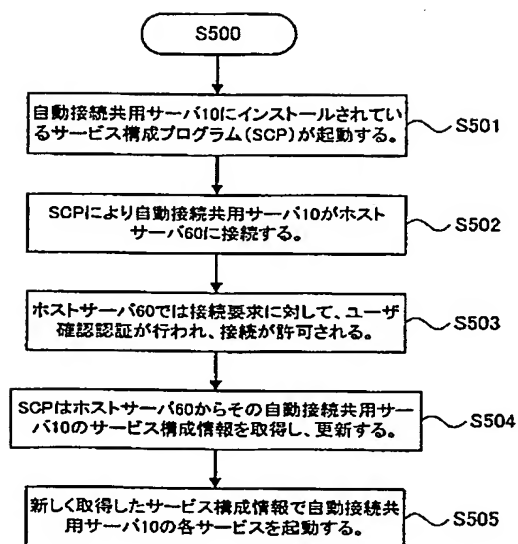
【図12】



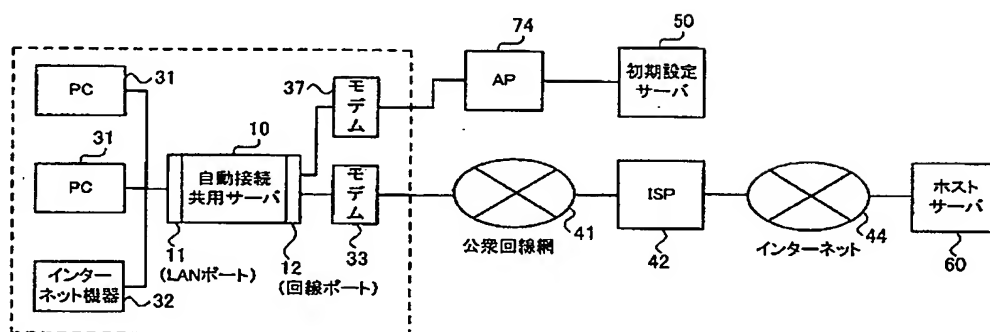
【図13】



【図14】



【図17】



フロントページの続き

Fターム(参考) 5B085 AE23 BC00  
 5B089 GA11 HA06 HA10 JB07 JB22  
 KA12 KA13 KB04 KB10 KC58  
 KG05 KG10  
 5K101 KK20 MM07 NN18 NN21 PP03  
 RR19 VV04